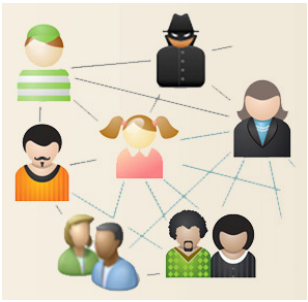
The Front Burner
Cyber Security

Office of the Chief Information Officer
Office of Cyber Security

Issue No. 10
August 2009

Social Networking Sites: How to stay safe!!



Social Networking sites, such as MySpace, Facebook, Twitter, Linkedin, refer to communities where one connects and communicates with others on the Internet. The extraordinary growth of social networking is altering the way people communicate, collaborate, and disseminate information; communication is accomplished using a variety of methods, such as email, blogging, texting, instant messaging or video/photo sharing. This enhanced world of connectivity is also blurring the lines between professional and private lives. As such, it is important to be mindful of the risks and potential impact of posting sensitive personal or work-related information. Remember, information posted on the Internet can live forever.

Below are some suggestions to protect yourself online while at work and at home:

- **Limit the amount of information you post** – Make sure you have management authorization to post any DOE-related information, and never post information identified as Classified, Official Use Only (OUO), Unclassified Controlled Nuclear Information (UCNI), or any sensitive personally identifiable information such as your Social Security number, credit card or bank information, date of birth, or mother's maiden name.
- **Evaluate the website privacy policies and service agreements** - Take advantage of a site's privacy settings. If you use a site that doesn't offer privacy settings, consider another site. The default settings for some sites may allow anyone to see your profile. You can often customize your settings to restrict access to only certain people. As a rule of thumb, don't post anything you wouldn't want seen now or in the future.
- **Use Strong Passwords** - Protect your account with passwords that contain a minimum of eight characters - a mix of upper and lower case letters, special characters and numbers, like 9P@$$worDz!. Use a different password than what you use at work.
- **Make sure your home computer is protected before visiting sites** – *Regularly Update the* anti-virus/anti-spyware and firewall software on your computer. Keep your operating system patched to the latest recommended level.
- **Do not assume that you are in a trusted environment** – Even on the personal web page of someone you know, it is still prudent to use caution when navigating and clicking on links or photos. Any content could have been compromised unknowingly and include malicious code or divulge your personal information.
- **Use your personal email address** – When you sign up for social networking sites for personal purposes, use a personal email address, not your work email address.
- **Review DOE Order 203.1** – Online access to social networking sites in the workplace is subject to the limited personal use restrictions as outlined in the order and organizational policies.
  You can find the order at: http://www.directives.doe.gov.

Are you Cyber Fit?

- ❒ Are you running anti-virus, anti-spyware, and a firewall on your home computer?
- ❒ Are you confident that your work and home passwords are safe, secure and strong?
- ❒ Do you know how to avoid phishing scams?
- ❒ Are you backing up your critical data often?
- ❒ Do you know what to do and who to contact if you suspect that your computer has a virus?
- ❒ Do you know how to protect your privacy on social networking sites?

If you answered "Yes" to all of these questions, we challenge you to come take the entire Cyber Fit Test at the "Takin' it to the Streets" cyber awareness event on August 19 at Forrestal. The first 50 DOE employees who score a 100% on the DOE Cyber Fit Test will each receive a Duffle bag!

DON'T MISS OUT ON THIS SUMMER'S "TAKIN' IT TO THE STREETS" CYBER SECURITY AWARENESS EVENT

The Department of Energy's Office of the Chief Information Officer is stepping up the pace at this year's *Takin' it to the Streets* cyber awareness event with activities and demonstrations to increase your cyber fitness. Raising our community's overall cyber awareness through good computing practices is essential for protecting us at work, at home, or wherever we connect to the online world.

If you're ready to get results, join the cyber fitness team and let us help you meet your cyber security goals.

OCTOBER EVENT

Are you an Internet Security Survivor?

Do you really know who you are talking to?
Are you protecting your personal information online?
Are you trashing e-mails from unknown senders?
Are you regularly updating your virus protection software?

An answer of **NO** to any of these questions can have serious security consequences, for you personally and possibly in the work place. Being an Internet Security Survivor requires judiciously practicing safe computing techniques at all times. The Internet is incredibly convenient for many activities, but with convenience comes risk – risk to your personal information and to sensitive government information. How do we protect ourselves personally as well as protect the government information with which we are entrusted? *By being aware of the risks **and** applying cyber security best practices.*

For important awareness information on how to survive in today's cyber space, please attend the **2009 Cyber Security Awareness Day being hosted at Forrestal on Thursday, October 22, 2009**. We are kicking off this year's event with an Internet Survivor Challenge to see who really knows how to practice safe computing. Teams from different DOE program offices will compete for prizes.

Stay tuned for more information about this exciting event in future Front Burner issues!!

Cyber Hero Answers Your Security Questions

Q: Can I limit who accesses my Social Networking profile?
A: It is possible to set profiles on some sites to "private" which should restrict access to only those individuals who have been granted permission to see it. Public profiles are generally available to anyone with access to the site. Make sure to read the terms of service and privacy policies and remember, what you publish on the Internet can live forever.

Q: **If I only have enough money to purchase either anti-virus or firewall software, which option should I choose**?
A: If you have limited funds, at least use the firewall that came with the operating system or a freeware version from a reputable vendor. Many Internet Service Providers also provide anti-virus/anti-spyware as part of your monthly service. Both a firewall and ant-virus software should be used to provide multiple levels of protection. Always remember, anti-virus is only as good as its last update. So choose a reputable vendor and update frequently.